UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/862,986	05/22/2001	Hezi Friedman	P04949 (NATI15-04949)	7516

7590 09/29/2006

William A. Munck
Novakov Davis & Munck, P.C.
13155 Noel Road, Suite 900
Dallas, TX 75240

EXAMINER	
ZAND, KAMBIZ	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 09/29/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.

EXAMINER

ART UNIT	PAPER
	20060926

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

Examiner Answer headings corrected based on the request by Appeal Center. A new examiner Answer using the proper headings is enclosed and forwarded to the BPAI.

KAMBIZ ZAND
PRIMARY EXAMINER

Kambiz Zand
Examiner
Art Unit: 2132

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/862,986
Filing Date: May 22, 2001
Appellant(s): FRIEDMAN ET AL.

William A. Munck
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 01/23/2006 appealing from the Office action mailed 08/23/2005 and 11/08/2005.

Real Party in Interest

(1) A statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings, which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments after Final

A statement identifying the status of amendments after Final is contained in the brief.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6216183

6,216,183	Rawlins	04-2001
5,799,196	Flannery	08-1998
2002/0141418	Ben-Dor et al.	10-2002
2002/0144115	Lemay et al	10-2002

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

1. **Claim 2** is rejected under 35 U.S.C. 103(a) as being unpatentable over Rawlins (6,216,183).

As per claim 2 Rawlins teach an apparatus for providing a secure serial bus (USB) comprising a secure channel for transferring data, wherein said apparatus comprises a secure USB domain device coupled to an external host computer, wherein said secure USB domain device comprises elements that are not accessible by said external host computer; a USB memory device that is not accessible by said host computer;

a USB processor that is not accessible by said host computer;

a USB host controller that is not accessible by said host computer; and

an internal USB bus that couples said USB memory device, said USB processor, and said USB host controller (see fig.1 and associated text; col.3, lines 8-40,48-50; col.1, lines 21-30; col.2, lines 20-31). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize the USB memory device, processor and host controller inaccessible to the host computer so as to prevent unauthorized access to data by a malicious computer user.

2. **Claims 8-10, 13 and 15** are rejected under 35 U.S.C. 103(a) as being unpatentable over Flannery (5,799,196) in view of Rawlins (6,216,183).

As per claims 8 and 15 Flannery teach an apparatus and method for providing a secure universal serial bus (USB) capable of transferring information over a secure channel, said apparatus comprising: at least one host computer capable of supporting USB input/output devices, said at least one host computer comprising a

USB bus, USB client software, and USB system software (see col.2, lines 5-18,12-15,18-22) but do not disclose explicitly a secure USB domain device capable of at least one of: blocking outgoing data flows of confidential information, forwarding outgoing data flows of encrypted confidential information, and forwarding outgoing data flows of non-confidential information. However Rawlins disclose a secure USB domain device capable of at least one of: blocking outgoing data flows of confidential information, forwarding outgoing data flows of encrypted confidential information, and forwarding outgoing data flows of non-confidential information (see col.2, lines 62-67 and col.3, lines 1-18). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Rawlins's USB secure device capable of blocking of confidential data in Flannery system in order to prevent leakage of the confidential information.

As per claim 9 Flannery teach all limitation of the claim as applied above but do not explicitly disclose wherein said secure USB domain device comprises:

a plurality of USB devices;

a first set of data channels for exchanging data with each of said plurality of USB devices; and

a second set of data channels for exchanging data with said at least one host computer. However Rawlins disclose the above limitation in fig.1 and associated text. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Rawlins's USB secure device capable of blocking of

confidential data in Flannery system in order to prevent leakage of the confidential information.

As per claim 10 Flannery teach an apparatus as claimed in Claim 8 wherein said secure USB domain device is embedded within said at least one host computer (see col.2, lines 12-14).

As per claim 13 Flannery disclose all limitation as applied above but do not explicitly disclose wherein said secure USB domain device is external to and coupled to said at least one host computer. However Rawlins disclose wherein said secure USB domain device is external to and coupled to said at least one host computer (see fig.1 and associated text; col.3, lines 8-18,48-50). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Rawlins's USB secure device capable of blocking of confidential data in Flannery system in order to prevent leakage of the confidential information.

3. **Claims 8-10, 13 and 15** are rejected under 35 U.S.C. 103(a) as being unpatentable over Flannery (5,799,196) in view of Rawlins (6,216,183) in further view of Ben-Dor et al (US2002/0141418 A1).

As per claim 20 Flannery in view of Rawlins teach all limitation of the claim as applied above but do not disclose coupling a virtual conduit interface to said secure

USB domain device; coupling said virtual conduit interface to at least one non-USB device, and using said virtual conduit interface to provide a secure USB channel for transferring information to said at least one non-USB device. However Ben-Dor et al disclose coupling a virtual conduit interface to said secure USB domain device; coupling said virtual conduit interface to at least one non-USB device, and using said virtual conduit interface to provide a secure USB channel for transferring information to said at least one non-USB device (see paragraph 73). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Ben-Dor's above limitation in Flannery in view of Rawlins in order to allow for the USB controller to interface with non-USB hardware.

4. **Claim 18** is rejected under 35 U.S.C. 103(a) as being unpatentable over Flannery (5,799,196) in view of Rawlins (6,216,183) in further view of Lemay et al (US2002/0144115 A1).

As per claim 18 Flannery teach all the limitation as applied above but do not disclose the wherein secure information is transferred between said at least one host computer and said secure USB domain device, thereby establishing at least one secure data channel between said at least one host computer and said secure USB domain device. However Rawlins disclose the wherein secure information is transferred between said at least one host computer and said secure USB domain

device, thereby establishing at least one secure data channel between said at least one host computer and said secure USB domain device (see col.3, lines 49-58). Flannery in view of Rawlins however do not disclose such transferring information is in ciphered format. Lemay et al disclose this on paragraph 58 and 59. Therefore it would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Lemay et al 's enciphering format features in Flannary in view of Rawlins to prevent the deciphering the information by an intruder.

As per claim 19 Flannery teach all limitations of the claim as applied above but do not disclose wherein data flows from a first device to a second device directly through said secure USB domain device without utilizing resources of said host computer. However Rawlins disclose wherein data flows from a first device to a second device directly through said secure USB domain device without utilizing resources of said host computer (see col.8, lines 25-32). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Rawlins utilization resources of said host computer in Flannery system in order to screen its outgoing flow and prevent access to the data from an unauthorized user.

(10) Response to Argument

Examiner makes the following remarks with respect to Appellant's arguments in order to simplify examiner's answer:

As per independent claim 2: Appellant's arguments that Rawling does not state "no accessibility is allowed during normal operation" page 7 last paragraph of the appeal brief is not persuasive since col.3, lines 7-26 clearly disclose during the normal operation such devices not accessible since it has to monitor target endpoint address of a USB device within the memory and such location only accessible during secure mode, therefore if such address (location) is not accessible during normal mode then how a USB device can be accessed when the address where it is found is not accessible (that is putting the address of the USB device into system memory 18 of the system 10). The problem with the appellant's arguments is that it is based on the wrong analogy, that the memory is within USB host controller 30. However the controller only transfer the target address of the USB device to the memory system 18 location. Therefore only authorized user that have access to the location of the memory may use the address of the target USB device in order to access it. Therefore the limitation "wherein said USB domain device comprises elements that are not accessible by said external host computer" is met since the domain is secure by providing only authorized access and not accessible otherwise. In support of examiner's above arguments, examiner refers to page 13 of the specification for support where a definition of secure domain creation is given and where it clearly states that two type data, one requires no intervention and the other do need intervention. In light of the page 13, fig.1 of the Rawling clearly disclose elements 32a-c as USB devices and system elements 12-30 creating the system in which the USB devices do communicate and where address for USB devices are

monitored within element 18 and if secure mode is not establish the address of the USB devices not accessible and therefore Rawling teach not accessibility of the USB devices by external system during the operation.

As per independent claim 8: Rawling do disclose in col.2, lines 62-67 and col.3, lines 1-25 exactly what appellant traversing. The limitation "blocking outgoing data flows of confidential information" is met by the fact that in secure mode the access to the USB device and the flow from USB device is block unless authorized. The limitation of forwarding outgoing data flows of encrypted confidential information and forwarding outgoing data flows on non-confidential information" is met by the fact that once the authorized access to a USB device by access to the address in memory 18 is given the flow of data (confidential or non confidential, encrypted or non-encrypted) is granted in either direction.

As per claim 9, Examiner only points out the limitations "first set of data channels" and "second set of data channels" only represent communication channels (BUSES) between the devices involved regardless of lexicon used by the Appellant. Fig. 1 of Rawlings discloses existence of the communication channels, which also is also known by one of ordinary skilled in the art as buses. Col.4, lines 49-51 describe the block diagram of fig.1 comprising various buses and bus interface units.

As per claims 10 and 13, the limitation "secure USB domain device is embedded within said at least one host computer" only represent the embedding of where the address for the USB device is located, that is the memory of the computer be embedded within so by using that address one can access USB devices that externally get connected to the computer. Col.1, lines 12-14 disclose above in broadest term since the computer is set to connect internally and externally. Furthermore such system also exists with Rawling in fig.1 in harmony with 103 rejections.

As per claim 15, Examiner points out that Applicant concede that Flannery disclose USB bus and software. Col.3, lines 7-26 clearly disclose during the normal operation such devices not accessible since it has to monitor target endpoint address of a USB device within the memory and such location only accessible during secure mode, therefore if such address (location) is not accessible during normal mode then how a USB device can be accessed when the address where it is found is not accessible (that is putting the address of the USB device into system memory 18 of the system 10). The problem with the appellant's arguments is that it is based on the wrong analogy, that the memory is within USB host controller 30. However the controller only transfer the target address of the USB device to the memory system 18 location. Therefore only authorized user that have access to the location of the memory may use the address of the target USB device in order to access it. In support of examiner's above arguments, examiner refers to page 13 of the specification for support where a definition of secure domain creation is given and where it clearly states that two type data; one requires no

intervention and the other do need intervention. In light of the page 13, fig.1 of the Rawling clearly disclose elements 32a-c as USB devices and system elements 12-30 creating the system in which the USB devices do communicate and where address for USB devices are monitored within element 18 and if secure mode is not establish the address of the USB devices not accessible and therefore Rawling teach not accessibility of the USB devices by external system during the operation.

As per claim 18 and 19 Lemay et al disclose on paragraph 58 and 59 transfer of information in enciphered format. Appellant do not dispute that fact but traverse the motivation of combining the references. However such motivation is reasonable since the enciphering/deciphering feature of Lemay adds to security of communication between USB devices and the host computer, because the secure USB device domain only protect the address for access to USB device, but when such access by authorized user is establish, then the question of secure communication is resolved by Lemay enciphering/deciphering capabilities in communication between two parties and therefore from the same environment that deals with secure access and communication, see paragraph [0040-0041] of Lemay which disclose USB environment in harmony with other references environment. Paragraph [0059] Lemay discloses the data transferred may be in encrypted (enciphered) format. Therefore it would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Lemay et al 's enciphering

format features in Flannary in view of Rawlins to prevent the deciphering the information by an intruder {0059} of Lemay

As per claim 20 Examiner makes the following remarks: USB bus driver is inherent part of USB device, or USB device would not work without it. Furthermore, in response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e." USB bus driver",) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Appellant traverses the motivation to combine with respect to claim 20 also not persuasive since Ben-Dor disclose tunneling between a bus and a network that is the communication channels between a BUS and other devices in the network and therefore in the same environment of network utilizing USB devices and secure domains. Paragraph [0073] of Ben-Dor disclose such harmony and environment in relation with other references combined. Motivation to combine also has support in paragraph [0074], which enables interface with other non-USB devices. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Ben-Dor's above limitation in Flannery in view of Rawlins in order to allow for the USB controller to interface with non-USB hardware.

In response to Appellant's arguments traversing motivation to combine, examiner makes the following remarks:

a) Lemay enciphering/deciphering capabilities in communication between two parties and therefore from the same environment that deals with secure access and communication, see paragraph [0040-0041] of Lemay which disclose USB environment in harmony with other references environment. Paragraph [0059] Lemay discloses the data transferred may be in encrypted (enciphered) format. Therefore it would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Lemay et al 's enciphering format features in Flannary in view of Rawlins to prevent the deciphering the information by an intruder {0059} of Lemay.

b) Ben-Dor disclose tunneling between a bus and a network that is the communication channels between a BUS and other devices in the network and therefore in the same environment of network utilizing USB devices and secure domains. Paragraph [0073] of Ben-Dor disclose such harmony and environment in relation with other references combined. Motivation to combine also has support in paragraph [0074], which enables interface with other non-USB devices. It would have been obvious to one of ordinary skilled in the art at the time the invention was

made to utilize Ben-Dor's above limitation in Flannery in view of Rawlins in order to allow for the USB controller to interface with non-USB hardware.

c) Rawlins disclose a secure USB domain device capable of at least one of: blocking outgoing data flows of confidential information, forwarding outgoing data flows of encrypted confidential information, and forwarding outgoing data flows of non-confidential information (see col.2, lines 62-67 and col.3, lines 1-18). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Rawlins's USB secure device capable of blocking of confidential data in Flannery system in order to prevent leakage of the confidential information. Appellant's focus on power management and not on other features of the Flannery is the problem of not recognizing the power management of Flannery do benefit other systems and methods of references used to combine, however it is the other features such as USB devices, its relationship with BUS, I/o connections that makes such motivation more proper, col.2, lines 5-18,12-15,18-22 disclose these features which corresponds to Applicant's invention environment. However it is Rawlings capabilities that add to other features of Flannery, by not only having the proper power management, which already exist in Flannery, but also adding Rawlings data blockage features in USB system of Flannery. Therefore such motivation is proper and It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Rawlins's USB secure device capable of blocking of

confidential data in Flannery system in order to prevent leakage of the confidential information.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

KAMBIZ ZAND
PRIMARY EXAMINER

Kambiz Zand

Primary Examiner

Art Unit 2132

September 26, 2006

Conferees

Kim Vu (SPE AU 2134)

Christopher A. Revak (Primary 2131)